symantec.

Norton™
Password Manager 2004

User's Guide

Norton™ Password Manager User's Guide

SYMANTEC LICENSE AND WARRANTY
Norton Password Manager

IMPORTANT: PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS THE INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU" OR "YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND SYMANTEC. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING THE "ACCEPT" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK THE "I DO NOT ACCEPT" OR "NO" BUTTON OR OTHERWISE INDICATE REFUSAL, MAKE NO FURTHER USE OF THE SOFTWARE AND CONTACT SYMANTEC CUSTOMER SERVICE FOR INFORMATION ON HOW TO OBTAIN A REFUND OF THE MONEY YOU PAID FOR THE SOFTWARE (LESS SHIPPING, HANDLING, AND ANY APPLICABLE TAXES) AT ANY TIME DURING THE SIXTY (60) DAY PERIOD FOLLOWING THE DATE OF PURCHASE.

1. License:

The software and documentation that accompanies this license (collectively the "Software") is the property of Symantec, or its licensors, and is protected by copyright law. While Symantec continues to own the Software, You will have certain rights to use the Software after Your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that Symantec may furnish to You. Except as may be modified by a Symantec license certificate, license coupon, or license key (each a "License Module") that accompanies, precedes, or follows this license, Your rights and obligations with respect to the use of this Software are as follows.

You may:

A. use one copy of the Software on a single computer. If a License Module accompanies, precedes, or follows this license, You may make the number of copies of the Software licensed to You by Symantec as provided in Your License Module. Your License Module shall constitute proof of Your right to make such copies;
B. make one copy of the Software for archival purposes, or copy the Software onto the hard disk of Your computer and retain the original for archival purposes;
C. use the Software on a network, provided that You have a licensed copy of the Software for each computer that can access the Software over that network;
D. after written notice to Symantec, transfer the Software on a permanent basis to another person or entity, provided that You retain no copies of the Software and the transferee agrees to the terms of this license; and
E. use the Software in accordance with any additional permitted uses set forth, below.

You may not:

A. copy the printed documentation that accompanies the Software;
B. sublicense, rent, or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;
C. use the Software as part of a facility management, timesharing, service provider, or service bureau arrangement;
D. use a previous version or copy of the Software after You have received a disk replacement set or an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed;
E. use a later version of the Software than is provided herewith unless You have purchased upgrade insurance or have otherwise separately acquired the right to use such later version;
F. use, if You received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which You have not received a permission in a License Module;
G. use the Software in any manner not authorized by this license; nor
H. use the Software in any manner that contradicts any additional restrictions set forth, below.

2. Content Updates:

Certain Software utilize content that is updated from time to time (including but not limited to the following Software: antivirus software utilize updated virus definitions; content filtering software utilize updated URL lists; some firewall software utilize updated firewall rules; and vulnerability assessment products utilize updated vulnerability data; these updates are collectively referred to as "Content Updates"). You shall have the right to obtain Content Updates for any period for which You have purchased maintenance, except for those Content Updates that Symantec elects to make available by separate paid subscription, or for any period for which You have otherwise separately acquired the right to obtain Content Updates. Symantec reserves the right to designate specified Content Updates as requiring purchase of a separate subscription at any time and without notice to You; provided,

however, that if You purchase maintenance hereunder that includes particular Content Updates on the date of purchase, You will not have to pay an additional fee to continue receiving such Content Updates through the term of such maintenance even if Symantec designates such Content Updates as requiring separate purchase. This License does not otherwise permit Licensee to obtain and use Content Updates.

3. Product Installation and Required Activation:

There are technological measures in this Software that are designed to prevent unlicensed or illegal use of the Software. You agree that Symantec may use these measures to protect Symantec against software piracy. This Software may contain enforcement technology that limits the ability to install and uninstall the Software on a machine to not more than a finite number of times for a finite number of machines. This License and the Software containing enforcement technology require activation as further set forth during installation and in the Documentation. The Software will only operate for a finite period of time prior to Software activation by You. During activation, You will provide Your unique product key accompanying the Software and PC configuration in the form of an alphanumeric code over the Internet to verify the authenticity of the Software. If you do not complete the activation within the finite period of time set forth in the Documentation, or as prompted by the Software, the Software will cease to function until activation is complete, which will restore Software functionality. In the event You are not able to activate the Software, You may contact Symantec Customer Support at the URL, or and telephone number provided by Symantec during activation, or as may be set forth in the Documentation.

4. Sixty (60) Day Money Back Guarantee:

If You are the original licensee of this copy of the Software and are not completely satisfied with it for any reason, please contact Symantec Customer Service for a refund of the money You paid for the Software (less shipping, handling, and any applicable taxes) at any time during the sixty (60) day period following the date of purchase.

5. Limited Warranty:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to You. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money You paid for the Software. Symantec does not warrant that the Software will meet Your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

6. Disclaimer of Damages:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC OR ITS LICENSORS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT, OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO CASE SHALL SYMANTEC'S OR ITS LICENSORS' LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether You accept the Software.

7. U.S. Government Restricted Rights:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are "Commercial Items," as that term is defined in 48 C.F.R. section 2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation," as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

8. Export Regulation:

The Software and its related documentation, including technical data, may not be exported or re-exported in violation of the U.S. Export Administration Act, its implementing laws and regulations, the laws and regulations of other U.S. agencies, or the export and import laws of the jurisdiction in which the Software was obtained. Export to any individual, entity, or country specifically designated by applicable law is strictly prohibited.

9. General:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England and Wales. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals, and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment, or similar communications between the parties. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. Software and documentation is delivered Ex Works California, U.S.A. or Dublin, Ireland respectively (ICC INCOTERMS 2000). This Agreement may only be modified by a License Module that accompanies this license or by a written document that has been signed by both You and Symantec. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write to: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, U.S.A., (ii) Symantec Authorized Service Center, Postbus 1029, 3600 BA Maarssen, The Netherlands, or (iii) Symantec Customer Service, 1 Julius Ave, North Ryde, NSW 2113, Australia.

This Software utilizes the Standard Template Library, a C++ library of container classes, algorithms, and iterators. Copyright © 1996-1999. Silicon Graphics Computer Systems, Inc. Copyright © 1994. Hewlett-Packard Company.

Contents

Feature summary

1

Use the information in this section to familiarize yourself with the product.

This section includes:

- A list of all of the features in the product
- A brief description of each feature

The feature summary can help you determine which feature to use to solve a problem. Read the feature descriptions to locate the correct component to use.

Activation protects you

Product activation is a technology that protects users from pirated or counterfeit software by limiting use of a product to those users who have acquired the product legitimately. Product activation requires a unique product key for each installation of a product. You must activate the product within 15 days of installing it.

Product activation is completely separate from registration. Your activation information and registration information reside on separate servers, with no link between the different sets of data.

When to activate your product

During installation, you are asked to enter a product key. After you have installed the product, activate it by sending the product key to the Symantec servers.

You can activate your product by clicking Activate Now in the Configuration Wizard that runs immediately after installation. If you choose not to activate at that time, you will receive *alerts* that will remind you to activate the product. You can click Activate Now in the alerts to activate the product. Activation should take just a few minutes.

If you do not activate the product within 15 days of installing it, the product will stop working. You can activate it after the 15 days have elapsed.

Locate the product key

The product key can most frequently be found on a sticker on your CD sleeve. If it is not there, then it will be on an insert in your product package. If you have purchased the product on DVD, look for the sticker on your DVD package. If you have *downloaded* the product from the Symantec Store, the product key is stored on your computer as part of the download process.

Norton Password Manager features

Norton Password Manager fills forms automatically and protects your passwords and other confidential information in encrypted files on your computer.

Norton Password Manager includes the following features:

A single profile password	You no longer need to remember passwords for all of the Web sites and programs that require them. After you have added your passwords and other information to a Norton Password Manager profile, you use a single profile password.
Password strength assistance	To ensure that your profile password is secure, a message appears if the password that you create is not strong.
Address and credit card wizard	The program steps you through the process of adding addresses, telephone numbers, and credit card information.
Privacy for shared computers	Norton Password Manager supports multiple profiles, all of which can have different passwords.
Secure portability	You can create backups of your profile data and restore the backups to another activated installation of Norton Password Manager.
Convenient access	When you are signed in to a profile, the Norton Password Manager icon appears in the Windows system tray for easy access when you need to sign in to a program or Web page.
Automatic updates	If program updates are issued, LiveUpdate retrieves and installs them automatically.

Installing Norton Password Manager

2

Before installing Norton Password Manager, take a moment to review the system requirements.

System requirements

To use Norton Password Manager, your computer must have one of the following Windows operating systems:

- Windows 98, 98SE/Me
- Windows 2000 Professional
- Windows XP Professional or Windows XP Home Edition

In Windows 2000/XP, you must have *Administrator access rights* to install Norton Password Manager and to run some features. If you are an Administrator and share your computer with others, remember that the changes you make apply to everyone who is using the computer.

Releases of Windows 95, Windows NT, and the server editions of Windows 2000 and Windows XP are not supported.

Your computer must also meet the following minimum requirements.

Operating system	System requirements
Windows 98/Me/ 2000 Professional	■ 133 MHz or higher processor ■ 32 MB of RAM (64 MB of RAM for Windows 2000 Professional) ■ 150 MB of available hard disk space ■ CD-ROM or DVD-ROM drive ■ Super VGA (800 x 600) or higher-resolution video adapter and monitor ■ Microsoft Internet Explorer 5.01 with Service Pack 2 or later (6.0 recommended)
Windows XP Home Edition/Professional	■ 300 MHz or higher processor ■ 128 MB of RAM ■ 150 MB of available hard disk space ■ CD-ROM or DVD-ROM drive ■ Super VGA (800 x 600) or higher-resolution video adapter and monitor ■ Microsoft Internet Explorer 5.01 with Service Pack 2 or later (6.0 recommended)

Prepare your computer

Before you install Norton Password Manager, prepare your computer.

If you have an earlier version of Norton Password Manager, the new version automatically removes the earlier version. You can transfer your existing information to the new version of the program.

Before you install Norton Password Manager, close all other Windows programs, including those programs displayed in the Windows system tray.

Install Norton Password Manager

You can install Norton Password Manager from the product CD or from a file that you downloaded.

To install Norton Password Manager

1 Do one of the following:
   - If you are installing from a CD, insert the CD into the CD-ROM drive.
   - If you downloaded your copy of Norton Password Manager, double-click the file you downloaded.

If your computer is not set to automatically open a CD, you will have to open it yourself.

2 Do one of the following:
   - In the Norton Password Manager CD window, click **Install Norton Password Manager**.
   - If you double-clicked a downloaded file, click **Install**.

3 In the Installation Wizard window, click **Next**.

4 In the License Agreement window, click **I accept the license agreement**, then click **Next**.
   If you decline, you cannot continue with the installation.

See "Activation protects you" on page 10.

5 In the Activation window, type the product key for activation, then click **Next**.

6 Do one of the following:
   - To confirm the default Destination Folder location, click **Next**.
   - To select a different Destination Folder, click **Browse**, then select another destination folder.

7 Click **Next**.

8 Review the summary of your installation selections, then click **Next**.
   The Setup window displays installation progress. Depending on your computer system speed, this can take a few minutes.

9 Scroll through the Readme file, then click **Next**.

10 In the Installation Complete message, click **Finish**. After installation, the Information Wizard will display a summary of installed settings.

11 If you are prompted to do so, click **Yes** to restart your computer.

After installation

In Windows 98/Me, you must restart your computer after installing Norton Password Manager. After it restarts, the Information Wizard steps you through product activation and registration and completes the installation setup.

Use the Information Wizard

The Information Wizard lets you activate your product, register your copy of Norton Password Manager, and update your program files using LiveUpdate.

🔱 If you choose not to register the software using the Information Wizard or if registration fails for some reason, you can register by using the Symantec Web site at www.symantec.com. On the Web site, go to the Products page for the registration link.

To use the Information Wizard

1 In the Norton Password Manager Information Wizard welcome window, click **Next**.

2 In the Product Activation window, click **Activate and register your product now**.

🔱 You must activate the software within 15 days.

3 Click **Next**.

4 Make sure that your computer is connected to the Internet, then click **Next**.

5   If you purchased your computer with Norton Password Manager already installed, you must accept the license agreement in order to use Norton Password Manager. Click **I accept the license agreement**, then click **Next**.

6   In the first Registration window, select the Country/Region from which you are registering.

7   If you would like information from Symantec about Norton Password Manager, check the method by which you want to receive that information, type the corresponding address and phone number, then click **Next**.

8   Check if you would like to receive postal mail from Symantec.

9   Type your name and address, then click **Next**.

10 Make sure your computer is connected to the Internet, then click **Next** to activate.

11 Click **Finish**.

12 Review the post-install tasks that Norton Password Manager will perform. These tasks include:

Create User Profile	Create a profile and master password so that you can start using Norton Password Manager.
	See "Set up a Norton Password Manager profile" on page 25.
Run LiveUpdate	If you are connected to the Internet, LiveUpdate can check for updated program files.
	See "Keeping current with LiveUpdate" on page 53.

13 In the Norton Password Manager Summary window, review your post-install tasks, then click **Finish**.

Read the Readme file

The Readme file contains technical tips and information about product changes that occurred after this guide went to press. It is installed on your hard disk in the same location as the Norton Password Manager product files.

To read the Readme file

1 Using Windows Explorer, navigate to the location where Norton Password Manager files are installed. If you installed Norton Password Manager to the default location, the files are in this path on your hard disk:
   C:\Program Files\Norton Password Manager

2 Double-click **Readme.txt** to open the file in Notepad, WordPad, or another word processing program.

Close the word processing program when you have finished reading the file.

If you need to uninstall Norton Password Manager

If you need to remove Norton Password Manager from your computer, you can use the Add/Remove Programs option from the Windows Control Panel.

During the uninstallation, Windows may indicate that it is installing software. This is a standard Microsoft installation message and can be disregarded.

To uninstall Norton Password Manager

1 Do one of the following:
   - On the Windows taskbar, click **Start** > **Settings** > **Control Panel**.
   - On the Windows XP taskbar, click **Start** > **Control Panel**.
2 In the Control Panel, double-click **Add/Remove Programs**.
3 In the list of currently installed programs, click **Norton Password Manager**.
4 Do one of the following:
   - In Windows XP/2000/Me, click **Change** or **Remove**.
   - In Windows 98, click **Add/Remove**.
5 In the Uninstall Norton Password Manager window, click **Next**.
6 If you want to delete your profile data, click **Yes**.
   If you click No, your encrypted profile data files will remain on your hard disk and can be used if you reinstall Norton Password Manager.
7 Click **Yes** to confirm that you want to uninstall the product.
8 Click **Finish** to restart your computer.

If you have no other Symantec products on your computer, LiveReg and LiveUpdate are also removed.

Basics

3

Basics include general information about how to:

- Work with your Symantec product.
- Keep your computer protected.
- Customize options.
- Monitor protection activities.
- Access more information.

Check the version number

You can check the version number of your product on your computer. Use the version number to help you find more information about your product on the Symantec Web site.

To check the version number

1 Start your product.
2 Click **Help and Support**.
3 On the Help menu, click **About <your product name>**.
4 In the About dialog box, select your product name.

Activate your product

Product activation reduces software piracy and ensures that you have received genuine Symantec software.

You must activate your product within 15 days of installing it or the product will stop working.

If you did not activate your product using the Configuration Wizard, you will receive an Activation Needed *alert* every day until you activate the product.

You can activate your product from the Activation Needed alert or from the Activation option on the Help menu. Activation should take just a few minutes.

To activate your product from the Activation Needed alert

1 In the alert, click **Activate Now**.
2 Click **OK**.
3 On the Activation screen, click **Next**.
4 On the Activation Successful screen, click **Finish**.

To activate your product from the Help menu

1 At the top of the main window, click **Help and Support** > **Activation**.
2 On the Activation screen, click **Next**.
3 On the Activation Successful screen, click **Finish**.

About profiles and passwords

The profile password is the key to using Norton Password Manager. It is very important that you choose a password that you can remember, but that is strong enough so that someone else can't guess it and gain access to your private information.

To set up a Norton Password Manager profile, you need a profile name, your country or region, and an optional profile password. The other information that is requested by the profile wizard, including name, addresses, and credit card information, is optional. The more information that is included in a profile, the less information you have to type when you are shopping online, or signing in to a program or Web site.

About profiles

The Norton Password Manager profile contains two types of information:

- ▪ The information that you add when you set up the profile, including a profile name, a profile password, your name, address, and credit card information. You can add or change the address and credit card information after the profile is created.

- ▪ The logon IDs and passwords that Norton Password Manager collects from Web sites and Windows programs. This list is associated with a specific profile. Once Norton Password Manager has recorded this information, it can sign in for you automatically, or provide more limited information if you prefer to sign in manually. You can delete Web sites and Windows programs from this list.

About strong passwords

A strong password is your best defense against identity theft. That is why it is important for you to create the strongest possible profile password. When you create a profile password, Norton Password Manager assists you.

If the password that you type is less than seven characters, Norton Password Manager displays a message that prompts you to type more characters.

A strong password has the following characteristics:

- At least seven characters
- At least one capital letter
- At least one lowercase letter
- At least one numeral (0 through 9)
- At least one symbol (for example, * ^ & $ %)

Although you can create a profile password with fewer characters, a longer password is more secure.

Set up a Norton Password Manager profile

To use Norton Password Manager you must create at least one profile. The only information that is required in a profile is a unique profile name and country or region. You can create multiple profiles, but you must set up each profile with this same setup process.

To make a profile useful, you should add as much information as possible to it. The information is safely stored on your computer in an encrypted format.

The setup process includes creating a strong profile password, and then adding other private information. Later, when you are browsing the Web or running Windows programs, you can add logon information for Web sites and programs that require you to log on. You must create a profile before you can begin using Norton Password Manager. You can add more information to a profile at any time.

To set up a Norton Password Manager profile

1 Do one of the following:
   - In the Windows system tray, right-click the Norton Password Manager icon, then click **Create New User Profile**.
   - In the Norton Password Manager main window, click **Status & Settings**, then click **Create Profile**.
     If you are signed in, click **Current Profile**, then click **New Profile**.

2 In the Profile Name window, type a unique name for the profile, select a country or region, then click **Next**.

If you have already created a profile and backed it up, you can restore its data to the new profile.

3 In the Password window, type a password, confirm the password by typing it again, then type a password hint. The hint should help you remember your password.

You can change a profile name or password later.

4 Click **Next**.

5 In the Identity window, type the name that you want to use for this profile, then click **Next**.
This name will be used to fill in Web and program forms.

6 In the Addresses section, type a home, work, or other address, then click **Next**.
Each profile can have up to three addresses. You can add information for a home, work, and other address. Each address can include a street address, phone and fax numbers, and an email address.
If you don't want to add addresses to the profile now, you can add them later.

7 In the Credit Cards section, add credit card information, then click **Next**. Your options are:

Card Type	Select the type, for example, Visa, MasterCard, Discover, American Express, or Other.
Card Description	Type a description that will help you identify this credit card.
Name on Card	Type the name as it appears on the credit card.
Card Number	Type the entire credit card number.
Expiration Date	Type the expiration date on the card.

Card Verification Number	Type the unique verification number for this card. This is usually located above the credit card number on the front of the card, or near the signature area on the back of the card.
Billing Address	Select the Home, Work, or Other address to which the credit card statement is sent.

8 To add another card, click **Add Another Card**.

If you don't want to add credit cards to the profile now, you can add them later.

9 In the Security Level window, select a security level, then click **Next**. Your options are:

High	You must type your profile password every time that you want to change any profile information. This option provides the highest level of security.
Medium	After you type your profile password, Norton Password Manager requests it again after the specified period of keyboard and mouse inactivity. This option protects you but does not cause you to type your profile password as frequently as the High option.
Low	You must type your profile password only once, when you sign in to a profile. This option is the least secure, in cases where your unattended computer might be used by someone else who could use your private information indiscriminately.

10 If you want to start using your profile right away, in the Setup Complete window, ensure that **Sign in to new profile now** is checked.

If you have signed into a profile, an alert box over the Windows system tray briefly displays the profile name.

11 Click **Finished**.

Access Norton Password Manager

You can start Norton Password Manager from the Windows Start menu, from a shortcut on the Windows desktop, and from an icon in the Windows system tray.

You can also close Norton Password Manager from the Windows system tray icon.

Start Norton Password Manager

From the Norton Password Manager main window you can use personal profiles, set options, run LiveUpdate, and perform other activities.

When Norton Password Manager is installed, its icon appears in the Windows system tray. You can access your profiles from here.

To start Norton Password Manager from the Windows system tray

1 In the Windows system tray, do one of the following:
   - Right-click the Norton Password Manager icon, then click **Open Norton Password Manager**.
   - Right-click the Norton Password Manager icon, then click **Sign In User Profile**.
2 In response to the confirmation message, click **Yes**.

To start Norton Password Manager from the Start menu or desktop

1 Do one of the following:
   - On the Windows taskbar, click **Start** > **Programs** > **Norton Password Manager** > **Norton Password Manager**.
   - On the Windows XP taskbar, click **Start** > **All Programs** > **Norton Password Manager** > **Norton Password Manager**.
   - On the desktop, double-click the Norton Password Manager icon.

2 In the Norton Password Manager main window, do one of the following:

- ◗ If you have not yet created a profile, click **Create Profile**.
- ◗ If you have already created a profile, click **Sign In**, select a profile, then type your password.

You must be signed in to a profile before you can view the status or options.

View a profile's status and settings

The Status & Settings window displays the status for the current profile.

To view a profile's status and settings

1 In the Norton Password Manager main window, click **Status & Settings**.

2 Select a feature to view its status. Your options are:

Current profile	The profile with which you signed into Norton Password Manager.
Passwords	The number of passwords that Norton Password Manager has for this profile. You can view details for this item.
Addresses	The number of addresses in the current profile. You can view details for this item.
Credit Cards	The number of credit cards in the current profile. You can view details for this item.
Security Level	The security setting in the profile. You can change this setting in the options or in the Security Level window.
Web Browser	Whether Norton Password Manager is monitoring Web sites. You can turn this setting on or off.
Windows Programs	Whether Norton Password Manager is monitoring Windows programs.

Close Norton Password Manager

Norton Password Manager normally starts with
Windows. You can close the program in the Windows
system tray.

To close Norton Password Manager

1 In the Windows system tray, right-click the Norton
   Password Manager icon, then click **Exit**.
2 In response to the confirmation message, click **OK**.
   To use Norton Password Manager again, you must
   start it from the Start menu.

Disable Norton Password Manager monitoring

You can disable Norton Password Manager monitoring of Web browsers and Windows programs. When these features are turned off, Norton Password Manager does not react when you open Web sites or Windows programs that require you to sign in. When these features are turned on, Norton Password Manager displays a dialog box when you open programs or Web sites that require you to sign in.

Any changes to Web and Windows program monitoring apply to the current profile.

To disable Web browser or Windows program monitoring

1 In the Norton Password Manager main window, click **Status & Settings**.
2 In the Status and Settings pane, under Monitoring Status, select one of the following:
   - Web Browser
   - Windows Programs
3 On the right side of the window, click **Off**.

Fill in forms with Norton Password Manager

You can use Norton Password Manager to automatically fill in Web forms and Windows programs with your private information. You can also use Norton Password Manager to select the data that you want to fill in manually. You can update and change your private information, including your addresses, telephone numbers, credit card information, and master password.

Because Norton Password Manager is available in the Windows system tray, it is available any time you want to add private information to an Internet form or Windows program.

About Internet forms

Norton Password Manager is designed to recognize most popular online forms.

Standard form fields include the following:

- First, middle, and last name
- Two address lines, for the street and suite number
- Phone number
- Email address
- Credit cards including Visa, MasterCard, American Express, Discover, and Diners Club

If a Web site form includes nonstandard information, Norton Password Manager cannot transfer the form data automatically with Quick Fill, but you can transfer it manually using Form Assistant.

Fill or ignore forms automatically

With your confirmation, Norton Password Manager automatically fills online transaction or shopping information, and inserts user names and passwords on password-protected Web pages and Windows programs.

Depending on the security level setting and the length of time that has elapsed since Norton Password Manager was used, you might need to type your profile password.

To fill or ignore Web forms automatically

1 In your browser, go to a Web site that requires you to type a personal ID or other personal data.

2 When Norton Password Manager asks if you want it to fill the form automatically, click **Fill Form**.
   If this is the first time that Norton Password Manager has seen the site, it offers to remember your ID and password if you enter them.

3 Do one of the following:
   - To add the information to the database, check **Yes**.
   - To ignore the form this time, check **No**.
   - To ignore the form permanently, check **Disable Quick Fill**, then click **No**.

If Norton Password Manager does not recognize the form, use Form Assistant to drag your private information into the Web site's text boxes.

To fill a Windows program automatically

1 Start the program where your private information is required.
   Norton Password Manager should recognize the empty form. If it does not recognize the form, you can use Form Assistant.

2 When Norton Password Manager asks if you want it to fill the form automatically, click **Fill Form**.
   The information in Norton Password Manager appears in the form.

3 If more information needs to be added manually, click **Go to Form Assistant**.

Fill forms manually

If a Web site or Windows program has a form that Norton Password Manager can't fill automatically, Norton Password Manager can assist you in filling the form so that you don't have to type the information again. Form Assistant displays the address and credit card

information from your profile so you can select the profile information that you need.

Using Form Assistant you can select and drag the text, such as a credit card number, to the corresponding text box in your Internet browser or Windows program.

To fill a form manually

1 In your Web browser, go to the Web site where your private information is required.
   The Form Assistant dialog box might appear automatically. If the Quick Fill dialog box appears, you can change to the Form Assistant.

2 Click **Go to Form Assistant**.
   You can also start Form Assistant by right-clicking the Norton Password Manager icon in the Windows system tray.

3 Click in the text box that contains the text that you need, for example, your name.

4 Drag the pointer to the destination text box in the browser or program, then release the mouse button.
   The text should appear in the destination Internet or program box.

5 If you need to change the information that appears in Form Assistant, click **Click here to edit profile options**.

Manage your profile information

Norton Password Manager includes a utility that backs up profile information to an external file. You can use this file as a safety backup, and to transfer your information to Norton Password Manager on a different computer.

Norton Password Manager encrypts all profile data files. The data that you back up cannot be read or decrypted by other programs.

Back up or restore your profile information

Norton Password Manager maintains your private profile data in a database. You can back up the profile by exporting the data to an external, encrypted file. You can also use this export/import feature to migrate your profile information to a different profile, or to another licensed installation of Norton Password Manager.

To back up the profile database

1 In the Norton Password Manager main window, click **Status & Settings** > **Current Profile**.
2 In the lower right of the window, click **Modify**.
3 On the left side of the Norton Password Manager Options dialog box, ensure that Profile Name is selected.
4 In the Profile Name dialog box, click **Backup Data**.
5 Type a file name, select the location for the backed-up file, then click **Save**.
6 Type a password that will be required to restore the backup.
7 Click **OK**.

⏻ If you do not want to overwrite the data in the current profile, you can add a new, empty profile, sign into it, and import the backup file to fill in the new profile data.

To restore the profile database

1 In the Norton Password Manager main window, click **Status & Settings** > **Current Profile**.
2 In the lower right of the window, click **Modify**.
3 On the left side of the Norton Password Manager Options dialog box, ensure that Profile Name is selected.
4 In the Profile Name dialog box, click **Restore Data**.
5 Click **Yes** to the warning that all data in the profile will be replaced.
6 Locate the backed-up file.
7 Click **Open**.
8 Type the password that was assigned to the backup, then click **OK**.

Create multiple profiles

You can create separate accounts in Norton Password Manager that have different master passwords. If you have created multiple accounts, you will be prompted to select the account that you want to use.

To create another profile

1 Do one of the following:
   - In the Windows system tray, right click the Norton Password Manager icon, then click **Create New User Profile**.
   - In the Norton Password Manager main window, click **New Profile**.
     If you are signed in, click **Current Profile**, then click **New Profile**.

2 Follow the setup wizard instructions to add a profile ID, password, name, address, and other private information.

The completed profile is added to the Norton Password Manager profile list.

Change to a different profile

If you have created more than one Norton Password Manager profile, you can select which one to use.

To change to a different profile

1 Do one of the following:
   - In the Windows system tray, right click the Norton Password Manager icon.
   - In the Norton Password Manager main window, click **Status & Settings** > **Current Profile**.
2 Click **Switch Profiles**.
3 In the Norton Password Manager Sign In dialog box, select another profile.
4 Type the password that is associated with the selected profile.
5 Click **Sign In**.

About the credit card verification number

Credit card companies include credit card verification numbers for extra security. Some companies require that you supply this number along with your credit card number.

The credit card ID number is usually located either above and to the right of the credit card number, or on the back of the card in the signature area. It is usually either four or seven digits long.

Set Norton Password Manager options

You can change the settings for the currently signed in profile in the Norton Password Manager Options dialog box. The following options are available:

Options	Enable or disable startup options.
	See "Set a profile's general options" on page 40.
Profile Name	Change a profile account name or region, or back up and restore profile data.
	See "Change profile information" on page 40.
Password	Change your profile password.
	See "Set up a Norton Password Manager profile" on page 25.
Identity	Change the name that is associated with this profile.
Addresses	Add, change, or remove a home, work, or other address.
	See "Change profile addresses" on page 42.
Credit Cards	Add, change, or remove a credit card.
	See "Change profile credit cards" on page 42.
Security Level	Change the security level for Norton Password Manager.
	See "Set Norton Password Manager options" on page 39.
Managed Passwords	View or remove the Windows programs and Web sites for which Norton Password Manager provides your password.
	See "View or delete managed passwords" on page 45.
Ignored Passwords	View or remove the Windows programs and Web sites for which Norton Password Manager does not provide your password.
	See "View or delete ignored passwords" on page 45.
Ignored Quick Fill Sites	View or remove Windows programs and Web sites.

Set a profile's general options

You can customize Norton Password Manager's startup settings, create profile backups, and restore profile data in the General Options dialog box.

To change Norton Password Manager general options

1 In the Norton Password Manager main window, click **Options**.
2 Your options are:

Startup Options	
	▪ Enable Norton Password Manager at startup: Norton Password Manager will respond if you sign in to a Web site or program.
	▪ Enable Web Browser support: Norton Password Manager will manage your passwords and fill in forms.
	▪ Enable Windows Program support: Norton Password Manager will sign in to Windows programs that require a password.
	▪ Enable Automatic LiveUpdate: LiveUpdate checks for and installs program updates without prompting you. LiveUpdate displays an alert when a program update has been downloaded.

Change profile information

Each Norton Password Manager profile must have a unique name. You can change the profile name and the country or region.

To change a profile name

1 In the Norton Password Manager main window, click **Status & Settings** > **Current Profile**.

2 In the lower right of the window, click **Modify**.

3 On the left side of the Norton Password Manager Profile Options dialog box, make sure that Profile Name is selected.

4 If you are prompted for a password, type it.

5 Make changes to the Profile Name.

6 Click **OK**.

You can also back up and restore profile data in this dialog box.

Change profile passwords

You can change the password for a profile.

To change a profile password

1 In the Norton Password Manager main window, click **Status & Settings** > **Current Profile**.

2 In the lower right of the window, click **Modify**.

3 On the left side of the Norton Password Manager Profile Options dialog box, click **Password**.

4 Click **more info** for advice on creating a strong password.

5 In the Password text boxes, type your old password, type a new password, confirm the password by typing it again, then type a password hint.

6 Click **OK**.

Change profile identity

You can change the name that is associated with this profile. This name is used to fill in Web forms and programs.

To change a profile identity

1 In the Norton Password Manager main window, click **Status & Settings** > **Current Profile**.

2 In the lower right of the window, click **Modify**.

3 On the left side of the Norton Password Manager Options dialog box, click **Identity**.

4 In the First Name, Middle Name, and Last Name text boxes, type the name that you want to use for this profile.

5 Click **OK**.

Change profile addresses

In Norton Password Manager you can add a home, work, and other address.

🔔 If you need to include additional addresses, consider creating a different profile.

To change a Norton Password Manager profile address

1 In the Norton Password Manager main window, click **Status & Settings** > **Addresses**.

2 In the lower right of the window, click **Details**.

3 Select an address type, for example, Home, Work, or Other.

4 In the address information dialog box, type the street address, phone and fax numbers, and your email address.

5 To change another address in this profile, select it and change the information.

6 Click **OK**.

Change profile credit cards

You can change the credit card for a profile.

To change a Norton Password Manager profile credit card

1 In the Norton Password Manager main window, click **Status & Settings** > **Credit Cards**.

2 In the lower right of the window, click **Details**.

3 Select the credit card that you want to change.

4 Change the available settings. Your options are:

Card Type	Select the type, for example, Visa, MasterCard, or American Express.
Card Description	Type a description that will help you identify this credit card.
Name on Card	Type the name as it appears on the credit card.
Card Number	Type the entire credit card number.
Expiration Date	Type the expiration date on the card.
Card Verification Number	Type the unique verification number for this card. This is usually located above the credit card number on the front of the card, or near the signature area on the back of the card.
Billing Address	Select the address to which the credit card statement is sent.

5 Click **OK**.

Change profile security level

You can change the frequency that Norton Password Manager requires you to sign in with your profile password.

To change the profile's security level

1 In the Norton Password Manager main window, click **Security Level**.
2 Change the available settings. Your options are:

High	You must type your profile password every time that you are prompted to enter any private information. This option provides the highest level of security.
Medium	After you type your profile password, Norton Password Manager requests it again after the specified period of keyboard and mouse inactivity.
	This option protects you but does not cause you to type your profile password as frequently as the High option.
Low	You must type your profile password only once, when you start Norton Password Manager.
	This option is the least secure, in cases where your unattended computer might be used by someone else who could use your private information indiscriminately.

View or delete managed passwords

When Norton Password Manager remembers a Web site password, the Web site is added to the managed passwords list. You can view or delete the Web sites on this list.

If you delete a site from the managed passwords list and then visit the site again, Norton Password Manager asks you if you want to remember the password again.

To view or delete a managed program or Web site

1 In the Norton Password Manager main window, click **Status & Settings** > **Passwords**.

2 On the left side of the Norton Password Manager Options dialog box, ensure that Managed Passwords is selected.

3 To remove a program or site from the list, select it, then click **Remove**.

4 Click **OK**.

View or delete ignored passwords

If you have specified that Norton Password Manager should not sign in to a program or Web site, it is added to the Ignored Passwords list. If you want Norton Password Manager to stop ignoring the program or site, remove it from the list.

To stop ignoring a program or Web site's password

1 In the Norton Password Manager main window, click **Status & Settings** > **Passwords**.

2 In the lower right of the window, click **Details**.

3 On the left side of the Norton Password Manager Options dialog box, click **Ignored Passwords**.

4 To remove a program or site from the list, select it, then click **Remove**.

5 Click **OK**.

View or delete ignored Quick Fill sites

If you want Norton Password Manager to fill in your profile information, remove the Web site or Windows program from the Ignored Quick Fill Sites list.

To view or delete an ignored Quick Fill site

1   In the Norton Password Manager main window, click **Status & Settings** > **Passwords**.

2   In the lower right of the window, click **Details**.

3   On the left side of the Norton Password Manager Options dialog box, click **Ignored Quick Fill Sites**.

4   To remove a program or site from the list, select it, then click **Remove**.

5   Click **OK**.

For more information

The product documentation provides glossary terms, online Help, a Readme file, the User's Guide in PDF format, and links to the Knowledge Base on the Symantec Web site.

Look up glossary terms

Technical terms that are italicized in the User's Guide are defined in the glossary, which is available in both the User's Guide PDF and Help. In both locations, clicking a glossary term takes you to its definition.

Use online Help

Help is available throughout your Symantec product. Help buttons or links to more information provide information that is specific to the task that you are completing. The Help menu provides a comprehensive guide to all of the product features and tasks that you can complete.

To use online Help

1   At the top of the main window, click **Help & Support** > **Norton Password Manager**.
2   In the Help window, in the left pane, select a tab. Your options are:

Contents	Displays the Help by topic
Index	Lists Help topics in alphabetical order by key word
Search	Opens a search field in which you can enter a word or phrase

Window and dialog box Help

Window and dialog box Help provides information about the program. This type of Help is context-sensitive, meaning that it provides help for the dialog box or window that you are currently using.

To access window or dialog box Help

❖ Do one of the following:
- ▪ In the window, click any available Help link.
- ▪ In the dialog box, click **Help**.

Readme file

The Readme file contains information about installation and compatibility issues. It also contains technical tips and information about product changes that occurred after this guide went to press. It is installed on your hard disk in the same location as the product files.

To read the Readme file

1 In Windows Explorer, double-click **My Computer**.
2 Double-click the hard disk on which you installed Norton Password Manager.
   In most cases, this will be drive C.
3 Click **Program Files** > **Norton Password Manager**.
4 Double-click **Readme.txt**.
   The file opens in Notepad or your default word processing program.
5 Close the word processing program when you are done reading the file.

Access the User's Guide PDF

The *Norton Password Manager User's Guide* is provided on the CD in PDF format. You must have Adobe Acrobat Reader installed on your computer to read the PDF.

If you purchased this product as an electronic download, Adobe Acrobat Reader was not included. You must download it from the Adobe Web site.

To install Adobe Acrobat Reader

1 Insert the CD into the CD-ROM drive.
2 Click **Browse CD**.
3 In the CD window, double-click the **Manual** folder.
4 Double-click the program file.
5 Follow the on-screen instructions to select a folder for Adobe Acrobat Reader and complete the installation.

Once you have installed Adobe Acrobat Reader, you can read the PDF from the CD.

If you do not have a CD, you can download the PDF from the Symantec Service & Support Web site.

To read the User's Guide PDF from the CD

1 Insert the CD into the CD-ROM drive.
2 Click **Browse CD**.
3 Double-click the **Manual** folder.
4 Double-click **NPM2004.pdf**.

You can also copy a User's Guide to your hard disk and read it from there.

To read a User's Guide from your hard disk

1 Open the location into which you copied the PDF.
2 Double-click the PDF.

Symantec products on the Web

The Symantec Web site provides extensive information about all Symantec products. There are several ways to access the Symantec Web site.

To access the Web site from the Help menu

❖ Select the solution that you want. Your options are:

Symantec Security Response	Takes you to the Security Response page of the Symantec Web site, from which you can update your protection and read the latest information about antithreat technology.
More Symantec solutions	Takes you to the Symantec Store Web site, from which you can get product information on every Symantec product.

To access the Symantec Web site in your browser

❖ On the Internet, go to www.symantec.com

Subscribe to the Symantec Security Response newsletter

Each month, Symantec publishes a free electronic newsletter that is focused on the needs of Internet security customers. It discusses the latest antivirus technology produced by Symantec Security Response, common viruses, trends in virus workings, virus outbreak warnings, and special *virus definitions* releases.

To subscribe to the Symantec Security Response newsletter

1 On the Internet, go to
   securityresponse.symantec.com

2 On the security response Web page, scroll down to the
   reference area of the page, then click **Newsletter**.

3 On the security response newsletter Web page, select
   the language in which you want to receive the
   newsletter.

4 On the subscribe Web page, type the information
   requested, then click **Subscribe**.

Keeping current with LiveUpdate

4

Symantec products depend on current information to protect your computer from newly discovered threats. Symantec makes this information available to you through LiveUpdate. Using your Internet connection, LiveUpdate obtains program updates and protection updates for your computer.

Your normal Internet access fees apply when you use LiveUpdate.

If your computer uses Windows 2000/XP, you must have Administrator *access privileges* to run LiveUpdate.

About program updates

Program updates are minor improvements to your installed product. These differ from product upgrades, which are newer versions of entire products. Program updates that have self-installers to replace existing software code are called patches. Patches are usually created to extend operating system or hardware compatibility, adjust a performance issue, or fix bugs.

LiveUpdate automates the process of obtaining and installing program updates. It locates and obtains files from an Internet site, installs them, and then deletes the leftover files from your computer.

About protection updates

Protection updates are files that are available from Symantec that keep your Symantec products up-to-date with the latest anti-threat technology. The protection updates you receive depend on which product you are using.

Norton AntiVirus, Norton AntiVirus Professional, Norton SystemWorks, Norton SystemWorks Professional, Symantec AntiVirus for Handhelds – Annual Service Edition	Users of Norton AntiVirus, Norton SystemWorks, and Symantec AntiVirus for Handhelds – Annual Service Edition products receive virus protection updates, which provide access to the latest virus signatures and other technology from Symantec.
Norton Internet Security, Norton Internet Security Professional	In addition to the virus protection updates, users of Norton Internet Security products also receive protection updates for Web filtering, intrusion detection, and Norton AntiSpam.
	The Web filtering protection updates provide the latest lists of Web site addresses and Web site categories that are used to identify inappropriate Web content.
	The intrusion detection updates provide the latest predefined firewall rules and updated lists of applications that access the Internet. These lists are used to identify unauthorized access attempts to your computer.
	Norton AntiSpam updates provide the latest spam definitions and updated lists of spam email characteristics. These lists are used to identify unsolicited email.
Norton Personal Firewall	Users of Norton Personal Firewall receive intrusion detection updates for the latest predefined firewall rules and updated lists of applications that access the Internet.
Norton AntiSpam	Users of Norton AntiSpam receive the latest spam definitions and updated lists of spam email characteristics.

Obtain updates using LiveUpdate

LiveUpdate checks for updates to all of the Symantec products that are installed on your computer.

If your *Internet service provider* does not automatically connect you to the Internet, connect to the Internet first, and then run LiveUpdate.

To obtain updates using LiveUpdate

1. At the top of the main window, click **LiveUpdate**.
2. In the LiveUpdate window, click **Next** to locate updates.
3. If updates are available, click **Next** to download and install them.
4. When the installation is complete, click **Finish**.

Some program updates may require that you restart your computer after you install them.

When you should update

Run LiveUpdate as soon as you have installed your product. Once you know that your files are up-to-date, run LiveUpdate regularly to obtain updates. For example, to keep your virus protection current, you should use LiveUpdate once a week or whenever new viruses are discovered. Program updates are released on an as-needed basis.

Set LiveUpdate to Interactive or Express mode

LiveUpdate runs in either Interactive or Express mode. In Interactive mode (the default), LiveUpdate *downloads* a list of updates that are available for your Symantec products that are supported by LiveUpdate technology. You can then choose which updates you want to install. In Express mode, LiveUpdate automatically installs all available updates for your Symantec products.

To set LiveUpdate to Interactive or Express mode

1 At the top of the main window, click **LiveUpdate**.

2 In the LiveUpdate welcome screen, click **Configure**.

3 In the LiveUpdate Configuration dialog box, on the General tab, select the mode that you want. Your options are:

Interactive Mode	Gives you the option of choosing which updates you want to install
Express Mode	Automatically installs all available updates

4 If you selected Express Mode, select how you want to start checking for updates. Your options are:

I want to press the start button to run LiveUpdate	Gives you the option of cancelling the update
I want LiveUpdate to start automatically	Installs updates automatically whenever you start LiveUpdate

5 To have access to a Symantec self-help Web site in the event that an error occurs while using LiveUpdate, check **Enable Enhanced Error Support**.

6 Click **OK**.

Turn off Express mode

Once you have set LiveUpdate to run in Express mode, you can no longer access the LiveUpdate Configuration dialog box directly from LiveUpdate. You must use the Symantec LiveUpdate control panel.

To turn off Express mode

1 On the Windows taskbar, click **Start** > **Settings** > **Control Panel**.

2 In the Control Panel window, double-click **Symantec LiveUpdate**.

3 In the LiveUpdate Configuration dialog box, on the General tab, click **Interactive Mode**.

4 Click **OK**.

Troubleshooting

5

Explore the Symantec service and support Web site

On the Symantec service and support Web site, you can find the latest protection and program updates, patches, online tutorials, Knowledge Base articles, and virus removal tools.

To explore the Symantec service and support Web site

1   On the Internet, go to www.symantec.com/techsupp

2   On the service and support Web page, under the heading home & home office/small business, click **Continue**.

3   On the home & home office/small business page, click **start online support**.

4   Follow the links to the information that you want.

If you cannot find what you are looking for using the links on the introduction page, try searching the Web site.

To search the Symantec service and support Web site

1   On the left side of any Symantec Web site page, click **search**.

2 On the search page, type a word or phrase that best represents the information for which you are looking. Use the following guidelines when searching the Symantec Web site:

- Type a single word in lowercase letters to find all occurrences of the word, including partial matches. For example, type install to find articles that include the word install, installation, installing, and so on.
- Type multiple words to find all occurrences of any of the words. For example, type virus definitions to find articles that include virus or definitions or both.
- Type a phrase enclosed in quotation marks to find articles that include this exact phrase.
- Type a plus (+) sign in front of all of the search terms to retrieve documents containing all of the words. For example, +Internet +Security finds articles containing both words.
- For an exact match, type the search words in uppercase letters.
- To search for multiple phrases, enclose each phrase in quotation marks and use commas to separate the phrases. For example, "purchase product", "MAC", "Norton SystemWorks" searches for all three phrases, and finds all articles that include any of these phrases.

3 Select the area of the Web site that you want to search.

4 Click **Search**.

Troubleshoot Norton Password Manager

Check here for suggestions to help solve problems that are encountered while you are running Norton Password Manager.

I'm using Netscape (or Opera) and my product won't work

Norton Password Manager works with Microsoft Internet Explorer version 5.01 SP2 and later only.

I've forgotten my master password

This version of Norton Password Manager does not provide any way of recalling or displaying your master password. It is encrypted and has other security measures to prevent unauthorized people from finding it in the program. It is not recorded anywhere except on your computer, so Symantec Technical Support representatives will not be able to provide it to you. If you can't remember your password, you will have to set up a new profile and retype your private information.

Service and support solutions

The Service & Support Web site at http://service.symantec.com supports Symantec products. Customer Service helps with nontechnical issues such as orders, upgrades, replacements, and rebates. Technical Support helps with technical issues such as installing, configuring, or troubleshooting Symantec products.

Methods of technical support and customer service can vary by region. For information on support offerings in your region, check the appropriate Web site listed in the sections that follow.

If you received this product when you purchased your computer, your computer manufacturer may be responsible for providing your support.

Customer service

The Service & Support Web site at http://service.symantec.com tells you how to:

- Subscribe to Symantec newsletters.
- Locate resellers and consultants in your area.
- Replace defective CD-ROMs and manuals.
- Update your product registration.
- Find out about orders, returns, or a rebate status.
- Access Customer Service FAQs.
- Post a question to a Customer Service representative.
- Obtain product information, literature, or trialware.

For upgrade orders, visit the Symantec Store at:
http://www.symantecstore.com

Technical support

Symantec offers two technical support options for help
with installing, configuring, or troubleshooting Symantec
products:

- Online Service and Support
  Connect to the Symantec Service & Support Web site
  at http://service.symantec.com, select your user type,
  and then select your product and version. You can
  access hot topics, Knowledge Base articles, tutorials,
  contact options, and more. You can also post a
  question to an online Technical Support
  representative.

- PriorityCare telephone support
  This fee-based (in most areas) telephone support is
  available to all registered customers. Find the phone
  number for your product at the Service & Support
  Web site. You'll be led through the online options
  first, and then to the telephone contact options.

Support for old and discontinued versions

When Symantec announces that a product will no longer
be marketed or sold, telephone support is discontinued
60 days later. Technical information may still be
available through the Service & Support Web site at:
http://service.symantec.com

Subscription policy

If your Symantec product includes virus, firewall, or Web
content protection, you may be entitled to receive
updates via LiveUpdate. Subscription length varies by
Symantec product.

After your initial subscription ends, you must renew it
before you can update your virus, firewall, or Web

content protection. Without these updates, you will be vulnerable to attacks.

When you run LiveUpdate near the end of your subscription period, you are prompted to subscribe for a nominal charge. Simply follow the instructions on the screen.

Worldwide service and support

Technical support and customer service solutions vary by country. For Symantec and International Partner locations outside of the United States, contact one of the service and support offices listed below, or connect to http://service.symantec.com and select your region under Global Service and Support.

Service and support offices

North America

Symantec Corporation
555 International Way
Springfield, OR 97477
U.S.A.

http://www.symantec.com/

Australia and New Zealand

Symantec Australia
Level 2, 1 Julius Avenue
North Ryde, NSW 2113
Sydney
Australia

http://www.symantec.com/region/
reg_ap/
+61 (2) 8879-1000
Fax: +61 (2) 8879-1001

Europe, Middle East, and Africa

Symantec Authorized Service Center
Postbus 1029
3600 BA Maarssen
The Netherlands

http://www.symantec.com/region/
reg_eu/
+353 (1) 811 8032

Latin America

Symantec Brasil
Market Place Tower
Av. Dr. Chucri Zaidan, 920
12° andar
São Paulo – SP
CEP: 04583-904
Brasil, SA

Portuguese:
http://www.service.symantec.com/br
Spanish:
http://www.service.symantec.com/mx
Brazil: +55 (11) 5189-6300
Mexico: +52 55 5322 3681 (Mexico DF)
01 800 711 8443 (Interior)
Argentina: +54 (11) 5382-3802

June 3, 2003

Glossary

access privileges	The types of operations that a user can perform on a system resource. For example, a user can have the ability to access a certain directory and open, modify, or delete its contents.
ActiveSync	The synchronization software for Microsoft Windows-based Pocket PCs.
ActiveX	A method of embedding interactive programs into Web pages. The programs, which are called controls, run when you view the page.
alert	A message that appears to signal that an error has occurred or that there is a task that requires immediate attention, such as a system crash or a Virus Alert.
alias	A shortcut icon that points to an original object such as a file, folder, or disk.
AppleTalk	A protocol that is used by some network devices such as printers and servers to communicate.
attack signature	A data pattern that is characteristic of an Internet attack. Intrusion Detection uses attack signatures to distinguish attacks from legitimate traffic.
beam	To transfer certain programs and data between two handheld devices using built-in infrared technology.

boot record	A sector at the start of a disk that describes the disk (sector size, cluster size, and so on). On startup disks, the boot record also has a program that loads the operating system.
bootable disk	A disk that can be used to start a computer.
cache	A location on your disk in which data is stored for reuse. A Web browser cache stores Web pages and files (such as graphics) as you view them.
cache file	A file that is used to improve the performance of Windows.
compressed file	A file whose content has been made smaller so that the resulting data occupies less physical space on the disk.
connection-based protocol	A protocol that requires a connection before information packets are transmitted.
connectionless protocol	A protocol that sends a transmission to a destination address on a network without establishing a connection.
cookie	A file that some Web servers put on your disk when you view pages from those servers. Cookies store preferences, create online shopping carts, and identify repeat visitors.
denial-of-service attack	A user or program that takes up all of the system resources by launching a multitude of requests, leaving no resources, and thereby denying service to other users.
DHCP (Dynamic Host Configuration Protocol)	A TCP/IP protocol that assigns a temporary IP address to each device on a network. DSL and cable routers use DHCP to allow multiple computers to share a single Internet connection.
dial-up	A connection in which a computer calls a server and operates as a local workstation on the network.

DNS (Domain Name System)	The naming system used on the Internet. DNS translates domain names (such as www.symantec.com) into IP addresses that computers understand (such as 206.204.212.71).
DNS server (Domain Name System server)	A computer that maps domain names to IP addresses. When you visit www.symantec.com, your computer contacts a DNS server that translates the domain name into an IP address (206.204.212.71).
domain	The common Internet address for a single company or organization (such as symantec.com). See also host name.
DOS window	A method of accessing the MS-DOS operating system to execute DOS programs through the Windows graphical environment.
download	To transfer a copy of a file or program from the Internet, a server, or computer system to another server or computer.
driver	Software instructions for interpreting commands for transfer to and from peripheral devices and a computer.
encryption	Encoding data in such a way that only a person with the correct password or cryptographic key can read it. This prevents unauthorized users from viewing or tampering with the data.
Ethernet	A common method of networking computers in a LAN (local area network). Ethernet cables, which look like oversized phone cables, carry data at 10M/100M/1G bps.
executable file	A file containing program code that can be run. Generally includes any file that is a program, extension, or system files whose names end with .bat, .exe, or .com.

extension	The three-letter ending on a file name that associates the file with an activity or program. Examples include .txt (text) and .exe (executable program).
FAT (file allocation table)	A system table (used primarily by DOS and Windows 9x/Me) that organizes the exact location of the files on the hard drive.
file type	A code that associates the file with a program or activity, often appearing as the file name extension, such as .txt or .jpeg.
Finder	The program that manages your Macintosh disk and file activity and display.
firewall rule	Parameters that define how a firewall reacts to specific data or network communications. A firewall rule usually contains a data pattern and an action to take if the pattern is found.
fragmented	When the data that makes up a file is stored in noncontiguous clusters across a disk. A fragmented file takes longer to read from the disk than an unfragmented file.
fragmented IP packet	An IP packet that has been split into parts. Packets are fragmented if they exceed a network's maximum packet size, but malicious users also fragment them to hide Internet attacks.
FTP (File Transfer Protocol)	An application protocol used for transferring files between computers over TCP/IP networks such as the Internet.
hidden attribute	A file attribute that makes files harder to access and more difficult to delete than other files. It also prevents them from appearing in a DOS or Windows directory list.
host name	The name by which most users refer to a Web site. For example, www.symantec.com is the host name for the Symantec Web site. Host names are translated to IP addresses by the DNS.

HotSync	The synchronization software for Palm OS handheld devices.
HTML (Hypertext Markup Language)	The language used to create Web pages.
ICMP (Internet Control Message Protocol)	An extension to the basic Internet Protocol (IP) that provides feedback about network problems.
IGMP (Internet Group Management Protocol)	An extension to the basic Internet Protocol (IP) that is used to broadcast multimedia over the Internet.
IMAP4 (Internet Message Access Protocol version 4)	One of the two most popular protocols for receiving email. IMAP makes messages available to read and manage without downloading them to your computer.
infrared (IR) port	A communication port on a handheld device for interfacing with an infrared-capable device. Infrared ports do not use cables.
IP (Internet Protocol)	The protocol that underlies most Internet traffic. IP determines how data flows from one computer to another. Computers on the Internet have IP addresses that uniquely identify them.
IP address (Internet Protocol address)	A numeric identifier that uniquely identifies a computer on the Internet. IP addresses are usually shown as four groups of numbers separated by periods. For example, 206.204.52.71.
ISP (Internet service provider)	A company that supplies Internet access to individuals and companies. Most ISPs offer additional Internet connectivity services, such as Web site hosting.
Java	A programming language used to create small programs called applets. Java applets can be used to create interactive content on Web pages.

JavaScript	A scripting language used to enhance Web pages. Most sites use JavaScript to add simple interactivity to pages, but some use it to open pop-up ads and reset visitors' homepages.
macro	A simple software program that can be started by a specific keystroke or a series of keystrokes. Macros can be used to automate repetitive tasks.
NAT (network address translation)	A method of mapping private IP addresses to a single public IP address. NAT allows multiple computers to share a single public IP address. Most DSL and cable routers support NAT.
network address	The portion of an IP address that is shared by all computers on a network or subnet. For example, 10.0.1.1 and 10.0.1.8 are part of the network address 10.0.1.0.
NTFS (NTFS file system)	A system table (used primarily by Windows 2000/XP) that organizes the exact location of all the files on the hard drive.
packet	The basic unit of data on the Internet. Along with the data, each packet includes a header that describes the packet's destination and how the data should be processed.
partition	A portion of a disk that is prepared and set aside by a special disk utility to function as a separate disk.
POP3 (Post Office Protocol version 3)	One of the two most popular protocols for receiving email. POP3 requires that you download messages to read them.
port	A connection between two computers. TCP/IP and UDP use ports to indicate the type of server program that should handle a connection. Each port is identified by a number.

port number	A number used to identify a particular Internet service. Internet packets include the port number to help recipient computers decide which program should handle the data.
PPP (Point-to-Point Protocol)	A protocol for communication between two computers using a dial-up connection. PPP provides error-checking features.
protocol	A set of rules governing the communication and transfer of data between computers. Examples of protocols include HTTP and FTP.
proxy	A computer or program that redirects incoming and outgoing traffic between computers or networks. Proxies are often used to protect computers and networks from outside threats.
registry	A category of data stored in the Windows registry that describes user preferences, hardware settings, and other configuration information. Registry data is accessed using registry keys.
removable media	Disks that can be removed, as opposed to those that cannot. Some examples of removable media are floppy disks, CDs, DVDs, and Zip disks.
router	A device that forwards information between computers and networks. Routers are used to manage the paths that data takes over a network. Many cable and DSL modems include routers.
script	A program, written in a scripting language such as VBScript or JavaScript, that consists of a set of instructions that can run without user interaction.
service	General term for the process of offering information access to other computers. Common services include Web service and FTP service. Computers offering services are called servers.

SSL (Secure Sockets Layer)	A protocol for secure online communication. Messages sent using SSL are encrypted to prevent unauthorized viewing. SSL is often used to protect financial information.
subnet	A local area network that is part of a larger intranet or the Internet.
subnet mask	A code, in the form of an IP address, that computers use to determine which part of an IP address identifies the subnet and which part identifies an individual computer on that subnet.
synchronize	The process by which a handheld device and computer compare files to ensure that they contain the same data.
TCP/IP (Transmission Control Protocol/ Internet Protocol)	Standard protocols used for most Internet communication. TCP establishes connections between computers and verifies that data is properly received. IP determines how the data is routed.
threat	A program with the potential to cause damage to a computer by destruction, disclosure, modification of data, or denial of service.
Trojan horse	A program containing malicious code that is disguised as or hiding in something benign, such as a game or utility.
UDP (User Datagram Protocol)	A protocol commonly used for streaming media. Unlike TCP, UDP does not establish a connection before sending data and it does not verify that the data is properly received.
virus definition	Virus information that an antivirus program uses to identify and alert you to the presence of a specific virus.

wildcard characters	Special characters (like *, $, and ?) that act as placeholders for one or more characters. Wildcards let you match several items with a single specification.
worm	A program that replicates without infecting other programs. Some worms spread by copying themselves from disk to disk, while others replicate only in memory to slow a computer down.

Index